

Subdomain takeover Explain

```
# subzy run --target swisscom.ch
# subzy run --targets subdomains.txt
```

- ثغره subdomain takeover بتحصل في حاله ان موقع معين يكون حاجز cloud وما يجددش اشتراكه
- في الحاله دي نت لو حجزته تقدر يكون ليك access علي الموقع ال كانو حجزين لي cloud
- بعد ما بتجمع subdomains بتشتغل باداه subzy

```
(root@kali)-[~]
# subzy run --targets file.txt --vuln --hide_fails
* ] Fingerprints found; checking integrity with an up
* ] Loaded 152 targets
* ] Loaded 76 fingerprints
No ] HTTPS by default (--https)
10 ] Concurrent requests (--concurrency)
No ] Check target only if SSL is valid (--verify_ssl)
10 ] HTTP request timeout (in seconds) (--timeout)
Yes ] Show only potentially vulnerable subdomains (--
```

- عندك --vuln-- hide_fails دا عشان ما بطلعش ليك غير المواقع او subdomains المصابه بس

| | | | | | |
|---------------|----------------|---|--------------|---|--|
| | | | | perfect! | |
| Readthedocs | Vulnerable | ■ | | The link you have followed or the URL that you entered does not exist. | Issue #16 |
| Sendgrid | Not vulnerable | ■ | | | |
| Shopify | Edge case | ■ | | Sorry, this shop is currently unavailable. | Issue #32 Issue #46 |
| Short.io | Vulnerable | ■ | | Link does not exist | Issue #26 |
| SmartJobBoard | Vulnerable | ■ | 52.16.160.97 | This job board website is either expired or its domain name is invalid. | Issue #13 |
| Smartling | Edge case | ■ | | Domain is not configured | Issue #67 |
| Smugsmug | Vulnerable | ■ | | | Issue #60 |
| Squarespace | Not vulnerable | ■ | | | |

- لو لقيت بتحط النوع ال ظهرك وتدور عليه هل ممكن تنفذ فيه الشغره ولا لا
- لان في انواع مش متاحه فيها الموضوع دا